Verwundbarkeitsanalysen mit OpenVAS

Herausforderungen der IT-Sicherheit

Einführung in OpenVAS

OpenVAS in Betrieb (nehmen)

Greenbone Networks GmbH

Produkt: Lösung für Schwachstellenscanning und -management

Gründung 2008 durch

- DN-Systems GmbH, Experten in IT-Sicherheit
- Intevation GmbH, Experten in Freie Software

Grundlagen:

- Durchgehend Freie Software (Open Source), GPLv2+
- OpenVAS
- Produktentwicklungen seit 2004, teilweise basierend auf gemeinsamen Projekten mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI)

Wirtschaftliche Bedeutung IT-Sicherheit

Schadensfall

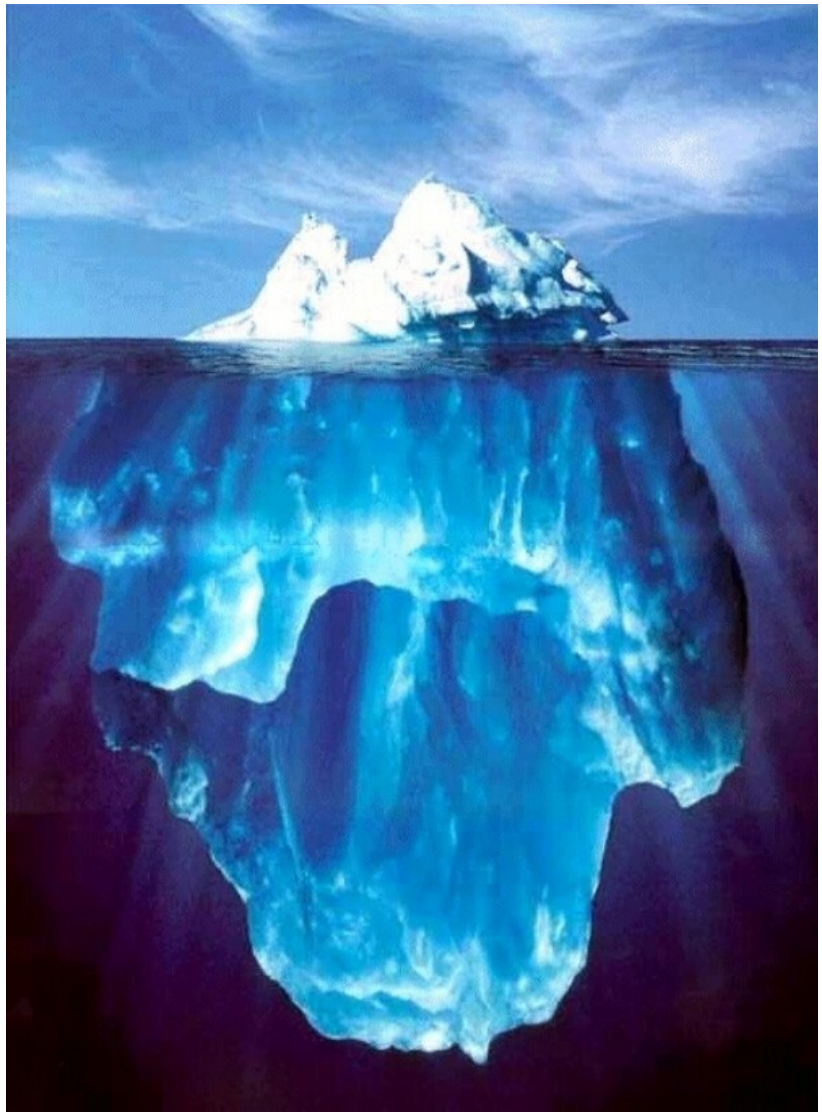
- Ausfall der Lieferung von Produkten, Dienstleistungen
- Kosten für Schadensbeseitigung
- Operative Verluste
- Reputationsverlust im Markt („brand poisoning“)
- Minderung der Verkaufszahlen, schwächere Marktposition

Nicht-Übereinstimmung mit gesetzlichen und regulatorischen Vorgaben/Richtlinien (Basel II, ISO 27001, FDCC, PCI, ...)

- Erhöhtes Risiko für Haftung
- Schlechtere Unternehmensbewertung

Wie groß ist das Sicherheitsproblem?

- Über 5.000 neue CVE Meldungen pro Jahr, insgesamt 40.000
- Glücklicherweise ist man nicht von allen allgemeinen Sicherheitsmeldungen betroffen
- Unglücklicherweise kennt man weder Zahl noch Art der Schwachstellen im eigenen Netz
- Unglücklicherweise finden Angriffe pauschal, automatisiert und täglich statt
- Präventive Schwachstellensuche muss holistischem Ansatz folgen:
  - Von Außen, von Innen und
  - Periodisch



Schwachstellen

Programmier- oder sonstiger Fehler öffnet einen Angriffsvektor

- In Geräten
- In Anwendungen
- In Betriebssystemen

Ordnungsgemäßes Schließen des Angriffsvektors über

- Patch/Update
- Rekonfiguration

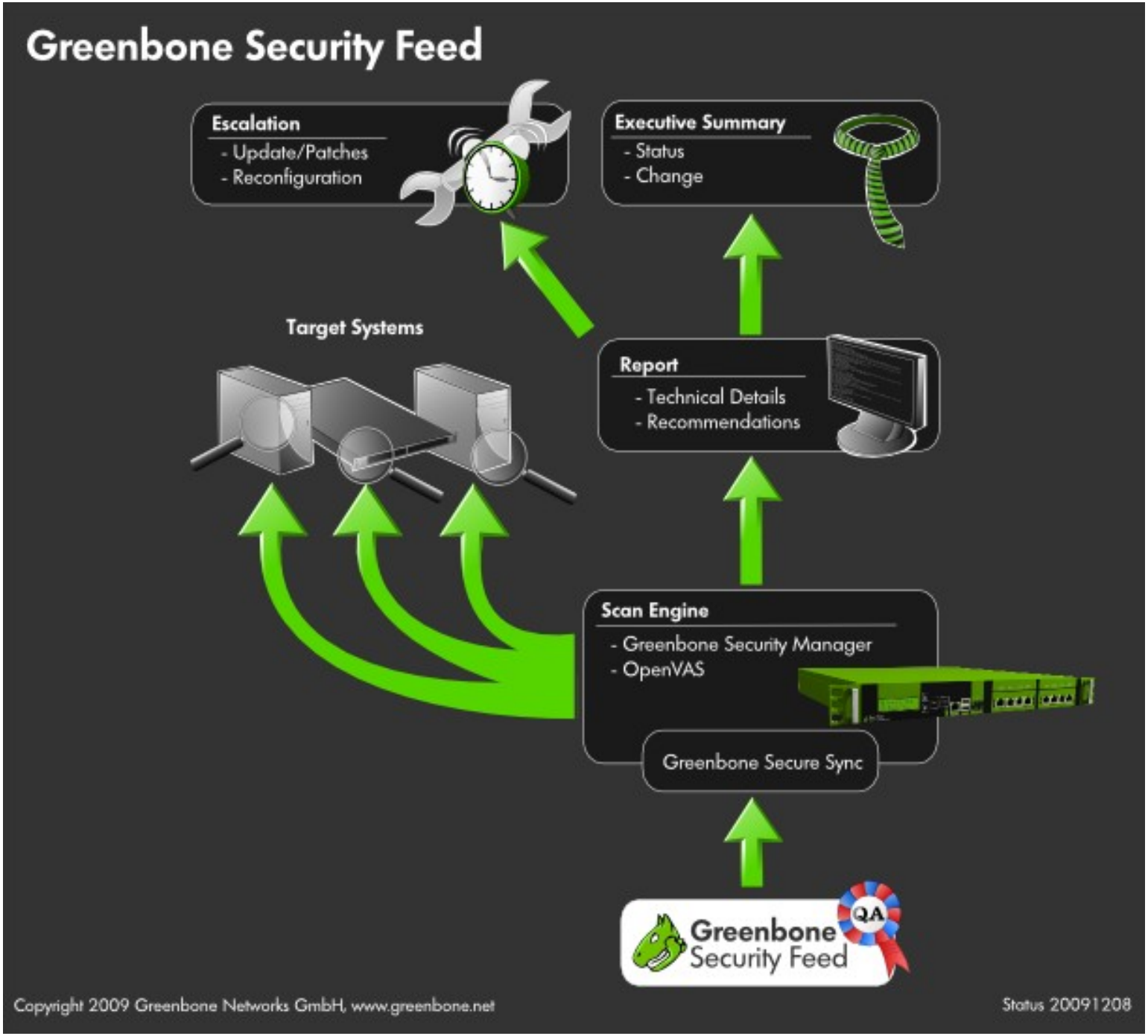
Workarounds über

- Port-Filter
- IDS
- Application-Filter

Schwachstellen-Scanning

Automatisierte Suche nach Angriffsvektoren

- Zu bekannten Schwachstellen werden Prüfroutinen erstellt
  - Täglich neue
  - Zentral verteilt („Feed“)
- Eine Scan-Engine (Vulnerability Scanner) führt die Prüfroutinen gegen Zielsysteme aus und erstellt Bericht über identifzierte Probleme
  - Es gibt False-Positives (Fehlalarm)
  - Es gibt False-Negatives (Fehlender Alarm)
- Schwachstelle vorhanden?
- Hersteller-Patch installiert? Auch wirksam?
- Anleitung, Hinweise zum schliessen des Angriffsvektors



Compliance

Compliance liegt vor bei Betrieb innerhalb definierter Parameter:

- Sicherheitsparameter (z.B. IT-Grundschutz, ISO 27001)
- Monitoringparameter (z.B. unternehmensinterne Sicherheitsrichtlinien)
- Gesetzliche Vorgaben (z.B. SOX)
  - Interpretiert durch Auditoren
  - Best practices
- Vertraglich definiert (z.B. PCI)

Durch Prüfung dieser Parameter wird analysiert ob Compliance weiterhin vorliegt oder Betriebsparameter angepasst werden müssen

Compliance

Prüfung auf Einhaltung von Sicherheits-Regelwerken umfasst:

- Systemparameter
  - Sicherheitseinstellungen für BS und Anwendungen
  - Änderung Sicherheitsstatus eines Parameters
- Handhabung unsicherer Altlasten
- Handhabung von Fehlkonfigurationen (entstanden durch Fehlbedienung oder durch Insider)
- Unsichere Passworte, unbenutzte Zugänge, ...

Beobachtung und Prüfung notwendig: Security-Audit

Schwachstellen-Management

„... ist der strukturierte Ansatz einen angemessenen Sicherheitsstatus der Unternehmens-IT zu gewährleisten“

Aspekte aus der Praxis

- Prüfung zur Wirksamkeit von Massnahmen
- Entwicklung Bedrohungsstatus über Zeit
- Scan-Iterationen
- Alarm-Trigger

Compliance (Einhaltung von Vorgaben)

- Assistenz (z.B. IT-Grundschutz)
- Unternehmenseigene Vorgaben (z.B. CPE-basierte Ge- oder Verbote)

OpenVAS ist der Open Source Vulnerability Scanner

- 2005: Abspaltung von Nessus
- 2006: Erste Entwicklerkonferenz (in Osnabrück)
- 2007: Aufbau Infrastrukturen, Code-Cleanups
- 2008: Version 1.0 (Feb), Start OpenVAS NVT Feed (Okt mit 5.800 NVTs), Version 2.0 (Dez)
- 2009: 10.000 NVTs (Apr), 2. Entwicklerkonferenz (Jul), 15.000 NVTs (Nov), 3.0-beta (Nov)

- Ca. 10 „SVN commits“ pro Tag
- Ca. 20 aktive Entwickler
- 5 Unternehmen die Support anbieten
- Ca. ??? Benutzer
  - In den meisten relevanten Linux-Distributionen
  - > 170.000 Primär-Downloads

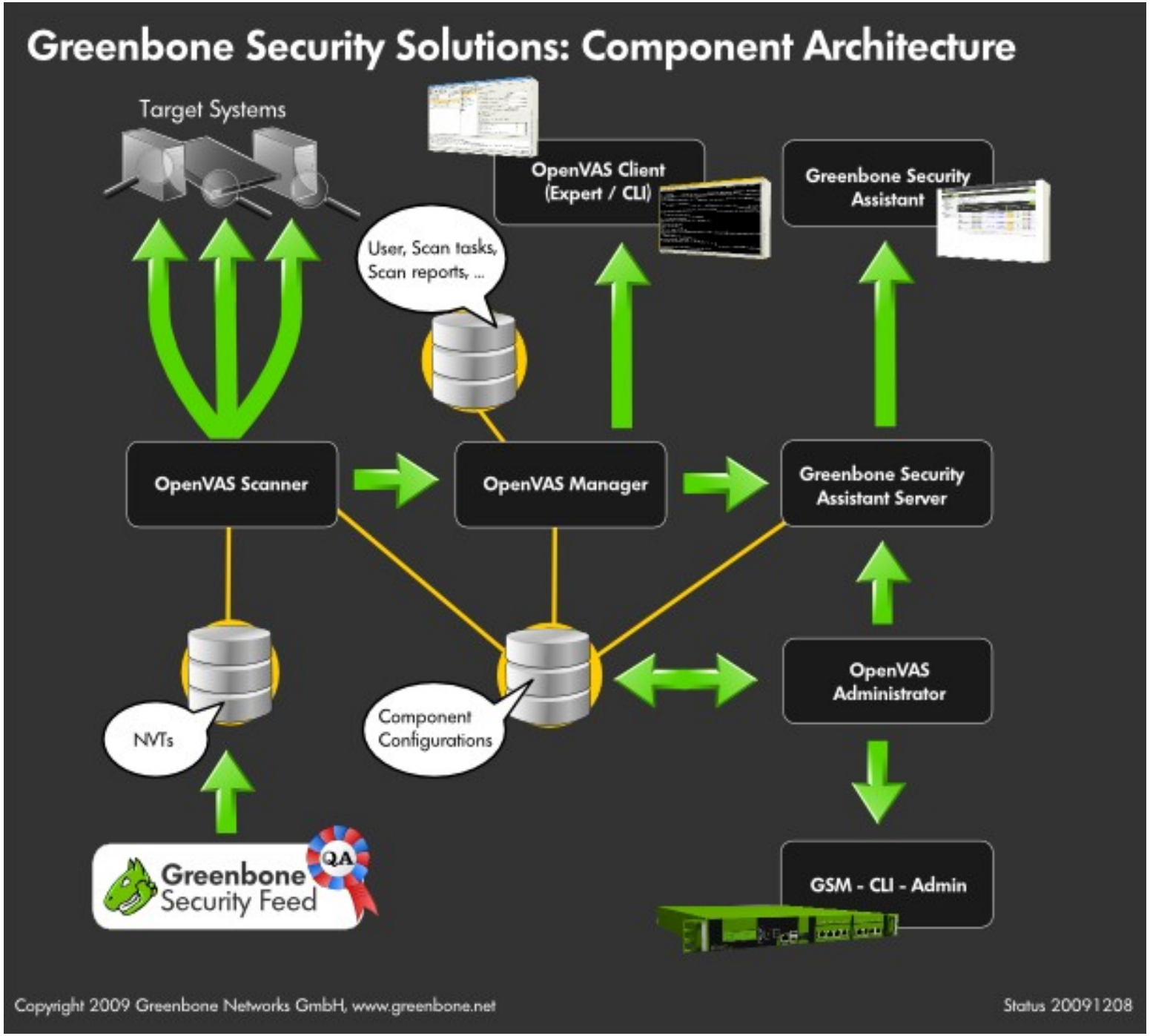
OpenVAS: Features und Eigenschaften

Features

- Scan-Methoden: Remote/Local Security Checks, Agenten-Tests
- Scan-Protokolle: WMI, SMB, LDAP, ...
- Security-Standards: CVE, CPE, OVAL, ...
- Integration: Nmap, ldapsearch, w3af, ovaldi, ...
- Reports: PDF, HTML, XML, NBE

Eigenschaften

- Implementiert in „C“, lizensiert unter GNU GPLv2
- Komponenten-orientierte Architektur
- Client-Server Architektur mit XML-basierten Protokollen (SSL!)
  - OTP: OpenVAS Transfer Protocol (noch kein XML)
  - OMP: OpenVAS Management Protocol
  - OAP: OpenVAS Administration Protocol



OpenVAS: Selbst gebaut

- Bau des Kerns der aktuellsten Version (3.0) aus Subversion:
  - Abhängigkeiten: Glib, GpgME, GNU/TLS, ...

```
$ cd $HOME
$ svn co https://svn.wald.intevation.org/svn/openvas/trunk
  openvas-trunk
$ mkdir install
$ export PATH=$HOME/install/sbin:$HOME/install/bin:$PATH
$ export LD_LIBRARY_PATH=$HOME/install/lib
$ cd openvas-trunk
$ (cd openvas-libraries ; ./configure –prefix=$HOME/install &&
  make install )
$ (cd openvas-scanner ; ./configure –prefix=$HOME/install &&
  make install )
$ (cd openvas-client ; ./configure –prefix=$HOME/install && make
  install )
```

OpenVAS: Selbst gebaut

Erweiterungen zu Version (3.0) aus Subversion:

```
$ (cd openvas-administrator ; cmake
  -DCMAKE_INSTALL_PREFIX=$HOME/install && make install )
$ (cd openvas-manager ; cmake
  -DCMAKE_INSTALL_PREFIX=$HOME/install && make install )
$ (cd gsa ; cmake -DCMAKE_INSTALL_PREFIX=$HOME/install && make
  install )
```

Start der Scan-Engine:

```
$ openvas-mkcert
$ openvas-adduser # oder openvasad –account=john:pass -r User
$ openvas-nvt-sync # dauert beim ersten mal
$ openvassd -p 9391 # dauert beim ersten mal
$ openvasad # optional
$ openvasmd -u # optional, dauert etwas
$ openvasmd # optional
$ gsad -p 8000 # optional
```

OpenVAS: Selbst gebaut

- Start des Desktop-Client:

```
$ OpenVAS-Client
```

- Start des CLI-Client:

```
$ OpenVAS-Client --config-file=myconf.openvasrc --output-
type=xml --batch-mode=localhost 9391 john pass targets.txt
results.txt

$ omp-cli -h localhost -p 9390 -u john -w pass --get-status
```

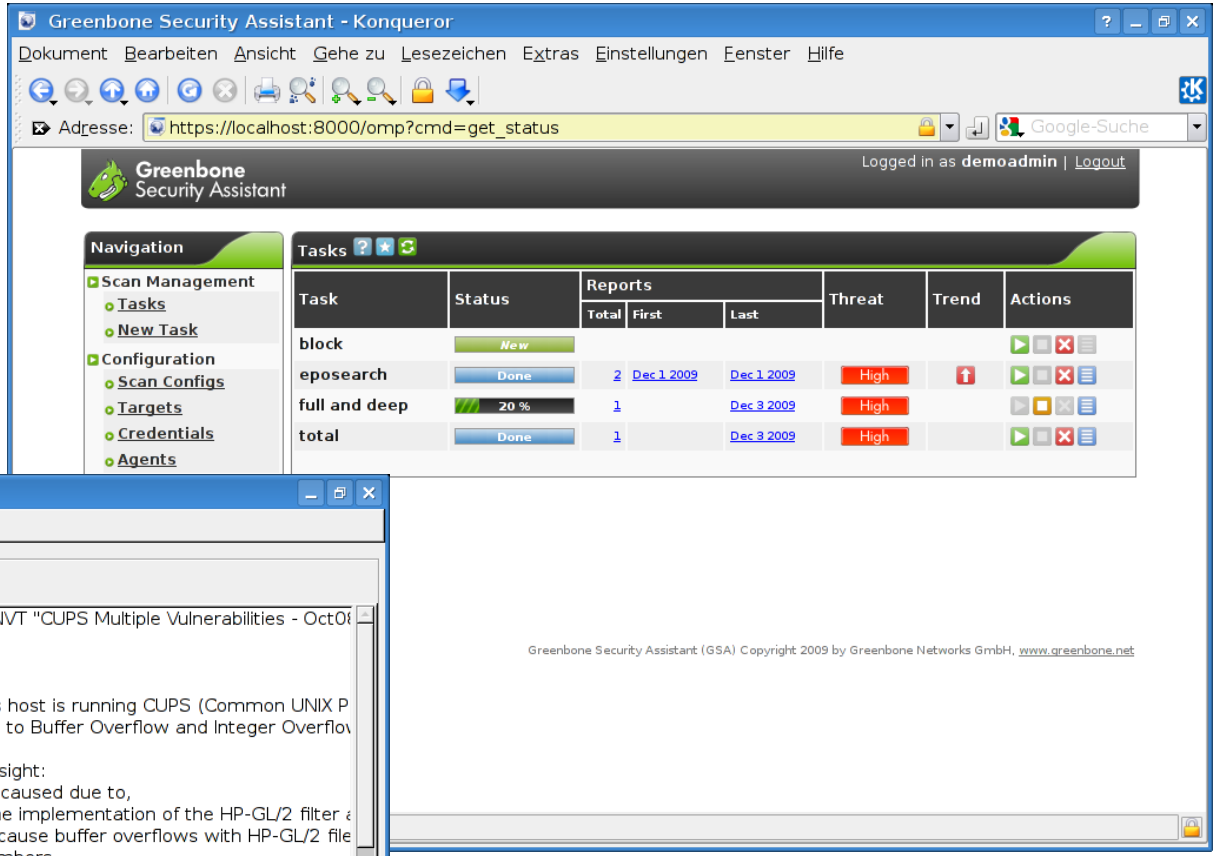
- Start des Web-Client:

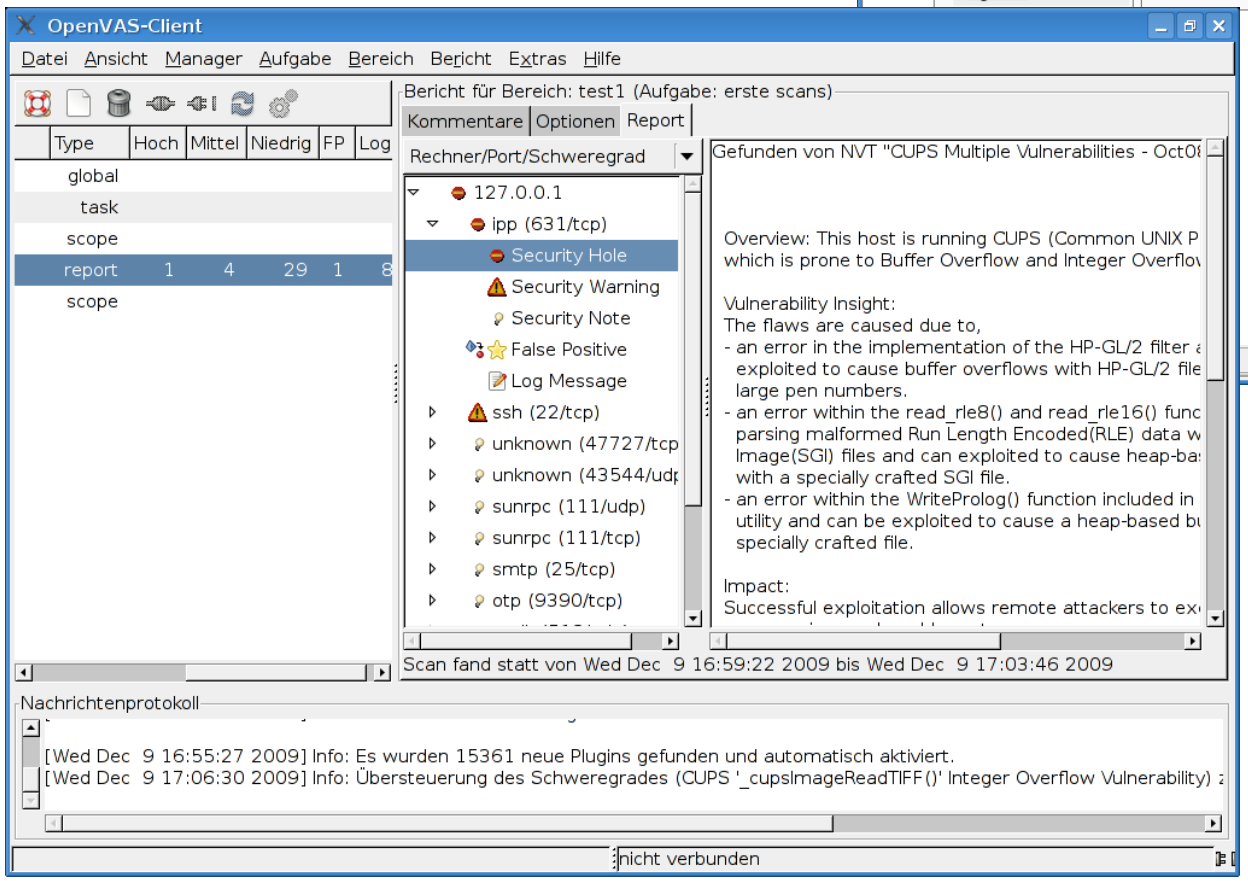
```
https://localhost:8000/
```

Live-Präsentation

Live-Präsentation

- OpenVAS-Client
- GSA





Vielen Dank für die Aufmerksamkeit!

Fragen?

Weitere Informationen:

- www.openvas.org
- Jan-Oliver.Wagner@greenbone.net
- www.greenbone.net